IN THE CLAIMS:

Amended claims follow:

1. (Currently Amended) A network adapter system, comprising:

(a) a processor positioned on a network adapter coupled between a computer and a network;

(b) wherein the processor is adapted for virus scanning and content scanning of network traffic transmitted between the computer and the network;

(c) wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data.

2. (Original) The network adapter system as recited in claim 1, wherein the processor is capable of being user-configured.

3. (Original) The network adapter system as recited in claim 2, wherein the processor is capable of being user-configured locally.

4. (Original) The network adapter system as recited in claim 2, wherein the processor is capable of being user-configured remotely via a network connection with the network adapter.

5. (Original) The network adapter system as recited in claim 2, wherein the processor is capable of being user-configured only after the verification of a password.

6. (Original) The network adapter system as recited in claim 2, wherein the manner in which the scanning is performed is capable of being user-configured.

7. (Original) The network adapter system as recited in claim 2, wherein the settings of the network adapter are capable of being user-configured.

8. (Original) The network adapter system as recited in claim 1, wherein the processor is capable of determining whether received packets are of interest.

9. (Original) The network adapter system as recited in claim 8, wherein the received packets are of interest based on an associated protocol.

10. (Original) The network adapter system as recited in claim 8, wherein the processor is capable of passing received packets that are not of interest to the computer.

11. (Original) The network adapter system as recited in claim 10, wherein the processor is capable of scanning received packets that are of interest.

12. (Original) The network adapter system as recited in claim 11, wherein the processor is capable of denying received packets that fail the scan.

13. (Original) The network adapter system as recited in claim 1, wherein the scan is performed based on user settings.

14. (Currently Amended) A method for scanning network traffic on a network adapter, comprising:

(a) receiving packets at a network adapter including a processor positioned thereon;

(b) virus scanning and content scanning of the packets utilizing the processor; and

(c) conditionally taking security measures if the packets fail the scan;

(d) wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data.

15. (Original) The method as recited in claim 14, wherein the processor is capable of being user-configured.

16. (Original) The method as recited in claim 15, wherein the processor is capable of being user-configured locally.

17. (Original) The method as recited in claim 15, wherein the processor is capable of being user-configured remotely via a network connection with the network adapter.

18. (Original) The method as recited in claim 15, wherein the processor is capable of being user-configured only after the verification of a password.

19. (Original) The method as recited in claim 15, wherein the manner in which the scanning is performed is capable of being user-configured.

20. (Original) The method as recited in claim 15, wherein the settings of the network adapter are capable of being user-configured.

21. (Original) The method as recited in claim 14, wherein the processor is capable of determining whether received packets are of interest.

22. (Original) The method as recited in claim 21, wherein the received packets are of interest based on an associated protocol.

23. (Original) The method as recited in claim 22, wherein the processor is capable of passing received packets that are not of interest to the computer.

24. (Original) The method as recited in claim 23, wherein the processor is capable of scanning received packets that are of interest.

25. (Original) The method as recited in claim 24, wherein the processor is capable of denying received packets that fail the scan.

26. (Original) The method as recited in claim 14, wherein the scan is performed based on user settings.

27. (Currently Amended) A system for scanning network traffic on a network adapter, comprising:

(a) network adapter means for receiving packets;

(b) processor means positioned on the network adapter means for virus scanning and content scanning of the packets; and

(c) means for conditionally taking security measures if the packets fail the scan;

(d) wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data.

28. (Currently Amended) A system for scanning network traffic on a network adapter, comprising:

(a) network adapter means for receiving packets;

(b) logic positioned on the network adapter means for virus scanning and content scanning of the packets; and

(c) logic for conditionally taking security measures if the packets fail the scan;

(d) wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data.

29. (Currently Amended) A network adapter system, comprising:

(a) a processor positioned on a network adapter coupled between a computer and a network, the processor including a packet assembly module, random access memory (RAM), and a scanner module;

(b) a user interface driver for identifying network traffic of interest transmitted between the computer and the network;

(c) wherein the processor is adapted for discerning and virus scanning and content scanning of network traffic of interest transmitted between the computer and the network

(d) wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data.

30. (New) The network adapter system as recited in claim 1, wherein the content scanning enforces operational policies of an organization.

31. (New) The network adapter system as recited in claim 30, wherein the policies include detecting entities selected from the group consisting of harassing content, pornographic content, junk e-mails, and misinformation.

32. (New) The network adapter system as recited in claim 1, wherein the virus signature files are stored on a non-volatile solid state memory on the network adapter.

33. (New) The network adapter system as recited in claim 32, wherein the memory is user protected by configuring a network adapter BIOS with a password that only a user can change.

34. (New) The network adapter system as recited in claim 11, wherein the received packets that are of interest include executable files.